Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Network Centric Operations

Challenges associated with the human-in-the-loop

Orrick White
Directorate of Science and Technology Policy

Defence R&D Canada – Ottawa
TECHNICAL REPORT
DRDC TR 2005-001
March 2005

Canada

105-05776/

Copy No: _____

Network Centric Operations

Challenges associated with the human-in-the-loop

Orrick White
Directorate of Science and Technology Policy

Defence R&D Canada

Technical Report

DRDC TR 2005-001

2005-03-07

Author

Orrick White

Approved by

Ingar Moen, PhD
Director of Science and Technology Policy

Approved for release by

Ingar Moen, PhD
Director of Science and Technology Policy

© Her Majesty the Queen as represented by the Minister of National Defence, 2005
© Sa majesté la reine, représentée par le ministre de la Défense nationale, 2005

Abstract

The human-system interface is central for achieving Network Centric Operations (NCO). Without systems that are designed to be human-centric, NCO will be a 'non starter'. Given this reality, studies of command and control compatibility between human operators and the network are crucial. Without this human oriented focus, unintended consequences will inevitably occur. Unfortunately, this would be just what the gurus of network centric operations were trying to overcome.

Résumé

L'interface homme-machine est cruciale aux opérations facilitées par réseaux. Sans système centré sur la personne, ces opérations seront vouées à l'échec. Les études sur la compatibilité en matière de commandement et contrôle entre les opérateurs humains et le réseau sont donc essentielles. L'absence de systèmes centrés sur la personne aura inévitablement des incidences non intentionnelles. Malheureusement, ces incidences étaient justement ce que les gourous des opérations facilitées par réseaux tentaient d'éliminer.

This page intentionally left blank.

Executive summary

In Canada, transformation is defined as "a departmental process of strategic re-orientation in response to anticipated or tangible change to the security environment, designed to shape our nation's armed forces to ensure their continued effectiveness and relevance." While transformation has been interpreted by some as being purely technological in nature, this is a false assumption. Instead, as the Canadian definition implies, transformation requires not only developing new technologies, but also operational concepts and organizational structures to conduct war in new ways.

One central transformational concept that has emerged in recent years is Network Centric Operations (NCO). NCO is an information superiority-enabled concept of operations that generates increased combat power by networking sensors and shooters to achieve shared awareness, increased speed of command, higher operational tempo, greater lethality, increased survivability, and a degree of self-synchronization.[1] In effect, NCO translates information superiority, into combat power by effectively linking knowledgeable entities in the sphere of operations.

While there have been many efforts to examine the technical challenges involved with the implementation of NEOps, there has been much less appreciation of the human dilemmas that networking will create. In general, we need to understand how people make decisions in complex environments and we need to develop a broader and more sophisticated understanding of what kind of machine-human interface networked systems will require in the years ahead.

White, O. 2005. Network Centric Operations: Challenges associated with the human-in-the-loop. DRDC TR 2004-010. DRDC DST Pol.

[1] In the United States, NEOps is referred to as Network Centric Warfare, or more recently Network Enabled Operations. In the UK, it is referred to as Network Enabled Capabilities. In NATO the preferred term is NATO Net Enabled Operations.

Sommaire

Au Canada, on définit la transformation comme un processus ministériel de réorientation stratégique attribuable à un changement prévu ou tangible de l'environnement de sécurité et servant à modeler les forces armées du pays pour en maintenir l'efficacité et la pertinence. Certaines personnes interprètent la transformation comme étant de nature purement technologique, mais il s'agit d'une hypothèse erronée. En effet, comme la définition canadienne le suggère, la transformation exige l'élaboration non seulement de nouvelles technologies, mais aussi de concepts opérationnels et de structures organisationnelles afin de parvenir à de nouvelles façons de faire la guerre.

L'opération facilitée par réseaux, un des concepts transformationnels essentiels ayant vu le jour au cours des dernières années, est un concept d'opération fondé sur la maîtrise de l'information qui produit une puissance de combat accrue grâce au réseautage des détecteurs et des tireurs, de façon à communiquer les connaissances et à augmenter la vitesse de commandement, le rythme des opérations, la létalité, la capacité de survie et l'autosynchronisation.[1] En fait, l'opération facilitée par réseaux transforme la maîtrise de l'information en une puissance de combat grâce à l'établissement de liens effectifs entre des entités bien renseignées de la sphère des opérations.

Si on a beaucoup étudié les défis techniques associés à la mise en œuvre des opérations facilitées par réseaux, on s'est beaucoup moins penché sur les problèmes humains que posera le réseautage. Il faut comprendre comment l'humain prend des décisions dans un environnement complexe et élargir et perfectionner notre compréhension du type de systèmes réseautés à interface homme-machine qui sera nécessaire dans les prochaines années.

White, O. 2005. Opérations facilitées par réseaux : Défis liés à l'intervention humaine. RDDC TR 2004-010. RDDC, DST Pol.

[1] Les États-Unis appellent les opérations facilitées par réseaux « guerre réseaucentrique », ou, plus récemment, « opérations réseaucentriques ». Le Royaume-Uni parle de « capacités facilitées par réseaux ». L'OTAN préfère, quant à elle, les nommer « opérations réseaucentriques », soit « Net Enabled Operations » en anglais.

Table of contents

Abstract i

Résumé i

Executive summary iii

Sommaire iv

Table of contents v

List of tables vi

Acknowledgements viii

Introduction 1

Network Centric Operations 3

Coalitions and Interoperability 5

Command and Control 6

Shared Situational Awareness and Understanding 7

Modelling and Simulation 9

Conclusion 11

References 112

List of symbols/abbreviations/acronyms/initialisms 13

List of tables

Table 1. From the Industrial Age to the Information Age v

Acknowledgements

The author would like to thank Dr. Ingar Moen and Dr. John Bovenkamp for their comments.

Introduction

> Despite military advances in military technology and the improvements in combat effectiveness that it promises, armed conflict ultimately remains a human endeavour. [2]
>
> The human element seems to underlie virtually all the functional shortcoming chronicled in official reports and media stories: information operations, civil affairs, cultural awareness, soldier contact, and most glaringly, intelligence, from national to tactical. [3]

Threats to security have changed in the 21st century. They are increasingly asymmetrical with impacts that in the historical sense are potentially vastly disproportionate to the effort invested. These threats can originate from complex and highly adaptive adversaries, and they can be initiated and supported from any place on the globe. Traditional military forces and purely defensive capabilities are no longer adequate in themselves to detect and neutralize threats, nor to provide long-term security. As a result of changes in the security environment, militaries around the world are attempting to transform their armed forces.

Military transformation is the act of creating and harnessing a revolution in military affairs. It requires developing new technologies, operational concepts and organizational structures to conduct war in new ways.[4] This involves: 1) orienting us towards emerging and future missions, 2) changing the way we operate in order to leverage information and technologies; and, 3) changing our business practices to take advantage of the information age.

In Canada, transformation has been defined as "a departmental process of strategic re-orientation in response to anticipated or tangible change to the security environment, designed to shape our nation's armed forces to ensure their continued effectiveness and relevance." While transformation has been interpreted by some as being exclusively technological in nature, against an enemy who fights unconventionally this view is false and downright dangerous.

---

[2] Directorate of Land Strategic Concepts. 2003. *Future Force: Concepts for Future Army Capabilities*. Kingston, Department of National Denfence. p 79.

[3] MGen Scales, Robert (Ret'd). 2004. "Culture Centric Warfare" in *Proceedings*. US Naval Institute. Oct. pp 32-41

[4] Binnendjijk, Hans. 2002. *Transforming America's Military*. Washington: National Defense University Press.

A central enabling concept of military transformation is Network Centric Operations.[5] While NCO involves technology, it is also about people, organisations and and nations being empowered to work together in new, more dynamic, flexible and effective ways. In order to achieve this, organisational and technological innovation and change must work hand-in-hand. Given this reality, this paper argues that the human-system interface is where the 'rubber hits the road' in Network Centric Operations. Without systems that are designed to be human-centric, NCO will be a 'nonstarter'.

In keeping with this view, the first section of the paper will discuss the essential elements of NCO while the remaining sections will address potential challenges and the areas of research and development that must be undertaken in order to make Network Centric Operations a possibility.

[5] Network Centric Operations (NCO), rather than network centric warfare, is the preferred term used in this paper as it has become quite clear that the scope of military operations goes much further than warfare.

Network Centric Operations

Network Centric Operations (NCO) is a product of the information age. It originally emerged in response to the different characteristics of warfare between the industrial age and information age as captured below. [6]

Table 1. From the Industrial to the Information Age

Industrial Age	Information Age
Massed Force	Dispersed Force
Info Based	Knowledge Based
Reactive	Proactive
Military Centric	Interagency Centric
De-conflicted Operations	Integrated Joint/Coalition Operations
Intermittent Pressure	Continuous Pressure
Precise Targeting	Precise Effects

In the information age, technology has compressed the time and space continuum. At the same time political realities have collapsed the clear separations among the strategic, operational and tactical levels by introducing more dynamic rules of engagement. NCO is intended to be a concept of operations that helps leverage the characteristics of the info age to enable military force to achieve effects based operations.[7]

NCO focuses on the combat power that can be generated from the effective linking or networking of the military enterprise. It is characterized by the ability of geographically dispersed forces to create a high level of shared battlespace awareness that can be exploited through self-synchronization to achieve commander's intent.[8]

NCO is an information superiority-enabled concept of operations that generates increased combat power by networking sensors and shooters to achieve shared awareness, increased speed of command, higher operational tempo, greater lethality,

---

[6] Ibid.

[7] Effects Based Operations (EBO) can be understood to be operations that focus on influencing behavior or capabilities using the integrated application of selected instruments of power. EBO entails the coordination of diplomatic, information, military and economic levers. Effects themselves can be physical or cognitive. This necessitates an understanding of friends', foes' and neutrals' perceptions -- hence, the emphasis on human factors and the interest in complex adaptive systems.

[8] Arthur K. Cebrowski and John J.Garstka, *Network Centric Warfare: Its Origin and Future*, Proceedings of the U.S. Naval Institute 124:1, (January 1998), 28-35.

increased survivability, and a degree of self-synchronization.[9] In effect, NCO translates information superiority, into combat power by effectively linking knowledgeable entities in the sphere of operations.

The assumptions on which NCO is based are: 1) a robustly networked force improves information sharing; 2) information sharing enhances the quality of information and shared situational awareness; 3) shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command; and 4) these, in turn, dramatically increase mission effectiveness.[10] In turn, the operational benefits that are expected to emerge from this are precision in applying force, rapidity of effect, a force multiplier effect, improved force protection, and improved combat effectiveness.

The operationalization of NCO will involve the provision of vastly increased access to information across all echelons and it will entail a redefinition of the role of a commander and the relationship between a commander, a commander's staff, subordinates, and superiors who are widely distributed geographically. NCO will have an impact on who has what information, how well the situation is understood, and the degree to which this understanding is shared.

---

[9] In the United States, NEOps is referred to as Network Centric Warfare, or more recently Network Enabled Operations. In the UK, it is referred to as Network Enabled Capabilities. In NATO the preferred term is NATO Net Enabled Operations.

[10] Network Centric Warfare. Department of Defense Report to Congress. July 2001. p1.

Coalitions and Interoperability

Due to the nature of the strategic environment in the 21st century, operations in the future will be joint, multinational, interagency and public (JIMP). Interoperability will be a more critical factor than ever before and it needs to occur simultaneously at a number of levels or layers to enable entities to communicate, share information and collaborate with one another. Participating entities will have to be connected to the network, be able to provide information to the network, and be able to find, retrieve, and understand the information available on the network.

NCO requires that coalition allies and national governments recognize that a critical mass of connectivity and interoperability is necessary to both encourage and support new ways of doing business. Networking the force is one of the top priorities of the US Department of Defence and they have committed significant funds for the development of a Global Information Grid (GIG) infrastructure. The role of the human in building this network will be essential because it will help determine how information is accessed and displayed. The development of intuitive interfaces is critical to shared awareness, especially across different organizations and coalition partners. It is expected that visualization, virtual displays and smart rooms, will facilitate the gathering of information throughout the grid and convert it to knowledge to achieve a consistent understanding of the sphere of operations.

That said NCO is based upon the ability of a force to develop shared situational awareness in the cognitive domain. Technical interoperability will get us to the point where the information is correctly represented in distributed systems, but does not ensure that the individuals in different locations, in different organizations, at different echelons have a similar understanding even though they "see" the same thing. With the added complexity of coalition operations that involve different cultures, the problem is greatly compounded. What is needed therefore, is semantic interoperability. Semantic interoperability is the capability to routinely translate the same information into the same understanding.

Command and Control

The success of any military operation relies upon command and control (C2) that brings about the necessary conditions for success. [11] In a networked force, command and control will not ultimately be the sole responsibility of any single individual. Instead, it will be shared, distributed and a collaborative responsibility and this distribution and devolution of authority devolution will require changes to command concepts and doctrine in the future. Coalition command and control is an area that merits special attention. Experience with coalition operations over the last decade shows that preconceived ideas of how operations will work do not necessarily pan out in practice. Instead of having one objective function to maximize, as in the case where a commander is clearly in charge, coalition operations involve multiple objective functions in a state of tension.

In order for the system to become truly knowledge-centric, the domains in which command during conflict takes place must be fully understood and the impact of networking appreciated by those who are in the face of battle.[12] Military entities and activities are located in four domains: the physical, information, cognitive, and social domains. The physical domain is where strike, protect and maneuver take place across the environments of sea, air, land and space; whereas, the information domain is where information is created, analysed, manipulated, value-added and shared. The cognitive domain is where the perceptions, awareness, understanding, decisions, beliefs and values of the participants are located and the social domain is where military force entities interact by exchanging information, awareness, understandings and making collaborative decisions. [13]

Cognitive activities by their nature are individualistic: they occur within the minds of individuals. However, shared sense-making, the process of going from shared awareness to shared understanding to collaborative decision-making, can be considered a socio-cognitive activity because an individual's cognitive activities are directly impacted by the social nature of the exchange. Our mental models, preconceptions, biases and values serve to influence how information is interpreted understood and acted upon. This is significant because an underlying assumption of NCO is that information sharing creates a common situational awareness.

---

[11] Pigeau and McCann, define Command as the creative expression of human will necessary to accomplish the mission and Control as those structures and processes devised by command to enable it. Pigeau, Ross and Carol McCann. "Re-Conceptualizing Command and Control" *Canadian Military Journal.* Vol 3, No 1 Spring 2002.

[12] Directorate of Land Strategic Concepts. 2003. *Future Force: Concepts for Future Army Capabilities.* Kingston, p. 99

[13] Alberts, David and Richard Hayes. 2003. *Power to the Edge. Available athttp://www.dodccrp.org , p. 113.*

While advanced technology allows users to collect information from diverse locations through the use of sensors deployed on both manned and unmanned platforms, it is a stretch to assume that the sharing of this information automatically guarantees a common operating picture. This is especially true if the information is distributed rather than co-located. The assumption that everyone will arrive at the same comprehension and projections based on the same information is often false because each individual interprets information in the context of their own beliefs and values.

Logically, in the context of multinational operations, this phenomenon becomes even more complex as cultural barriers to teamwork involving both organizational and cognitive aspects have been shown to arise. A recent study of multinational operations found that culture influences the cognitive fundamentals of teamwork, such as communication, coordination, understanding and decision-making.[14] Culture also influences the organizational barriers through national rules and procedures for training and personnel selection.

Shared Situation Awareness and Understanding

The ability to achieve a heightened state of shared situational awareness and knowledge among all elements of a joint force, in conjunction with allied and coalition partners (interoperability), is increasingly viewed as a cornerstone of transformation. A network enable operational situation must included the disposition of forces, capability of forces, analysis of possible courses of action, analysis of the environment, inferences of threat intentions for near, mid and long term periods of time, and network security status. Emerging evidence from recent military operations and a broad range of experimentation supports the relationship between shared situational awareness, knowledge, and increased combat power.

Understanding how sensemaking occurs is important for achieving a shared situational awareness. Sensemaking encompasses the range of cognitive activities undertaken by individuals, teams, organizations, and indeed societies to develop awareness and understanding and to relate this understanding to a feasible battlespace. According to experts, a major research effort is needed to explore the issues in sensemaking, the factors that influence our sense-making abilities, and how it relates to military situations.[15] The bulk of sense-making performance at the individual, team, and organization levels falls largely within the cognitive domain. However, sensemaking in military operations involves streams of decision events that occur simultaneously over different functional areas.

---

[14] Curts, R.J. and D.E. Campbell. 2003. *Cultural Barriers To Teamwork in a Multinational Coalition Environment.* Paper presentation at the 23rd Army Science Conference in Orlando, Florida.
[15] Alberts, David. 2001. *Information Age Transformation. Washington: CCRP, pp 136-138.*

Key aspects of human and organizational behaviors still need to be determined in order to help us understand and manage complex networks, and ensure the quality of information, collaboration, awareness, and shared situational awareness (including awareness of social and cultural issues). This is important because shared awareness and understanding will have a direct impact on the type of decisions that the end user makes based on the information provided.

Command and control systems lie at the heart of NCO, but many of the systems use classical analytic decision-making paradigms as their principal design foundation. This reflects the influence of prescriptive models of automated command decision-making. Unfortunately, the operational environment is a highly complex and unstructured environment to which prescriptive models cannot be easily transferred.

While classical approaches to decision making are based on the premise that human decision-making can be modelled on formal processes predicted by theories of probability, rationality and logic, over the past fifteen years, researches have recognized that the conditions of the battlefield place limitations on the human decision maker's ability to follow a truly analytic approach. Individuals are likely to deal with multiple pieces of information that may be ambiguous, highly unrelated with obscured or missing parts. Studies have shown that even expert decision-makers tend to consider only a few potential solutions when solving complex real-world problems. Real world situations often demand very rapid responses and decision makers may have to accept a solution that merely works without considering whether or not a better solution exists.[16] This reality is not necessarily incorporated into the rational models.

[16] To learn more about this refer to Bryant, David et al. 2003. "Synthesizing Two Approaches to Decision making in Command and Control" *Canadian Military Journal. pp* 29-34.

Modelling & Simulation: Enabling NCO

As militaries continue to transform into networked forces they are facing challenges that include: personnel recruitment for an increasing operational tempo, acquisition of new systems resulting in entirely new capabilities, changes to the threat environment and increased pressure to plan, acquire, and train defence capability in a joint context, and the need to complete acquisition and training processes faster and to a higher level of quality. Modeling and simulation (M&S), through the use of synthetic environments, may be key for developing our understanding of many of these complex interactions. It may also be useful for visualizing the operation of the system-of-systems as a whole and its interaction with other lines of development. As identified by the Canadian Department of Defence, M&S offers several benefits:

- The ability to test prototype or concept systems before constructing them, including measuring the performance of real operators;
- The ability to perform experiments that would be dangerous, environmentally sensitive, and /or cost-prohibitive using real equipment;
- The ability to run complex and sophisticated experiments and analysis more quickly and cheaply than by other methods, and to perform the experiments many times in a cost-effective manner; and,
- The ability to test different versions of the same system sequentially and rapidly under the exact same environment conditions, scenario, terrain and manning.[17]

Overall, it is anticipated that M&S will facilitate a faster and more complete evaluation of concepts at an earlier phase of their development. Moreover, the 'unity of thought' that comes form a shared, joint, synthetic environment will further increase the quality of informed decision making.

While M&S has several benefits, there are also some hurdles associated with the level of complexity that synthetic environments must grapple with when modeling complex environments. As a recent paper by Curts and Campbell states, the major technical goal of the next ten years will be the utilization of an architecture that allows interoperability between operational C4I systems and M&S efforts so that operators can train on the same systems that they will use in the field using M&S.[18] The initial steps at linking simulations and operational systems include programs that focus on establishing a common taxonomy between C4I systems and simulations, establishing web-based services for linking tactical databases to

[17] Department of National Defence. 2004. *The Joint Simulation and Modelling for Analysis, Requirements, Training, and Support (SMARTS) Initiative: A Vision for enabling Strategy 2020 though the application of Modelling and Simulation in DND.* Ottawa, p 8.

[18] Curts, R.J. and D.E. Campbell. 2003. Architecture: The Foundation of Coalition Interoperability and the Road to Information Assurance. NATO RTO SCI-137 Symposium on Architectures for Network-Centric Operations. Athens Greece, 20-22 October.

simulations and using software agents to track and monitor changes in the common operational picture.

Directly related to the above, many note that NCO raises fundamental systems of systems engineering issues associated with the design, acquisition, integration and support of the complex socio-technical systems.[19] These challenges include:

- Creating an environment in which we can investigate and evolve future concepts enabled by NCO – including analysis, experimentation and simulation.
- Managing the complexity associated with a network enabled system including integration, management, configuration, interoperability with legacy and peer systems and future migration.
- Developing the means to optimize the system to support the needs of the commander while exploiting the innate capability of the human in the system to maximum effect.
- Providing the analytic framework to model the socio-technical system, including an adequate representation of cognition and team interactions, justifying the necessary balance of investment in enablers/soft elements.

Challenges also exist in the provision of resilient network infrastructure to underpin NCO, particularly in complex environments (such as urban operations). The increasing use of adaptive and reconfigurable systems in the sphere of operations will raise fundamental safety, critical design and vulnerability management issues. Unfortunately, the ability to model cyber threats including interruption of service, denial of service, corruption of information, dissemination of information and hacking is in its infancy at this time.

Finally, the design of data mining, fusion and inference techniques will continue to be a priority area for research, as we struggle to identify key indicators in the wealth of data collected by increasingly numerous and distributed sensors. Because humans have a finite ability to deal with amounts of data and information developing techniques for information 'push' versus information 'pull' will be necessary.

[19] The Technical Cooperation Program (TTCP). 2004. *NAMRAD Principals Action Group on Network Centric Warfare. Final Report*. 23 February.

Conclusion

In closing, there is little doubt that the adoption of a network centric approach can fundamentally change the way militaries train and conduct operations, however as demonstrated above, there are major challenges that must be tackled before this transformation becomes a reality. Challenges exist across many dimensions, but fundamentally the most difficult ones seem to be related to human factors and the socio-cognitive domains.

While NCO advocates have typically focused on the technological aspects, in fact, doctrine, training, acquisition processes as well as many other aspects of the military are affected by adopting a NCO approach. Given the 'sea change' of operations in the information age, we can expect that there will be cultural resistance due to indoctrinated belief systems, values and ideas.

Ultimately, this should not be surprising since conflict is in the final analysis a "clash of human will(s)". While a host of factors influence the character or means involved in the conflict, it is the cognitive and physical manifestations that actually create and drive conflict and/or cooperation. Given this reality, attempts to overcome the challenges facing the adoption of NCO must also place the individual at the center.

References

Alberts, David. 2002. *Information Age Transformation. 2nd ed.* Washington: CCRP

Alberts, David, John Gartska and Frederick Stein. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority.* Washington: CCRP.

Bowman, Elizabeth and Linda Pierce. 2002. *Cultural Barriers to Teamwork in a Multinational Coalition Environment.* Paper presentation at the 23rd Army Science Conference in Orlando.

Curts, R.J. and D.E. Campbell. 2003. *Architecture: The Foundation of Coalition Interoperability and the Road to Information Assurance.* NATO RTO SCI-137. Athens, Greece.

Directorate of Land Strategic Concepts (DLSC). 2003.*Future Force: Concepts for Future Army Capabilities.* Kingston, Ontario.

DoD. 2001. *Network Centric Warfare. Department of Defence Report to Congress.* March.

Department of National Defence. 2004. *The Joint Simulation and Modelling for Analysis, Requirements, Training, and Support (SMARTS) Initiative: A vision for enabling Strategy 2020 though the application of Modelling and Simulation in DND.* Ottawa, Ontario.

Febrache, David. 2004. Strategic Defence Review – New Chapter. Presentation at the TTCP Multinational Workshop on Network Warfare. DRDC Valcartier. 10-13 February.

Menken, Thomas and James FitzSimonds. 2003. *The Limits of Transformation.* Rhode Island: Naval War College Press.

Scales, MGen Robert (Ret'd). 2004. "Culture Centric Warfare" in *Proceedings.* US Naval Institute. OCT. pp 32-41.

The Technical Cooperation Program (TTCP). 2004. *NAMRAD Principals Action Group on Network Centric Warfare. Final Report.* 23 February.

List of symbols/abbreviations/acronyms/initialisms

C2	Command and Control
EBO	Effects Based Operations
DND	Department of National Defence
GIG	Global Information Grid
M&S	Modelling and Simulation
NCO	Network Centric Operations

DOCUMENT CONTROL DATA SHEET

1a. PERFORMING AGENCY
Defence R&D Canada

2. SECURITY CLASSIFICATION
Unclassified/Unlimited

1b. PUBLISHING AGENCY
Defence R&D Canada

3. TITLE
Network Centric Operations: Challenges associated with the human-in-the-loop

4. AUTHORS
Orrick White, Directorate of Science and Technology Policy

5. DATE OF PUBLICATION
March 2004

6. NO. OF PAGES
28

7. DESCRIPTIVE NOTES

8. SPONSORING/MONITORING/CONTRACTING/TASKING AGENCY
Sponsoring Agency: Defence R&D Canada

9. ORIGINATORS DOCUMENT NO.
DRDC-TR-2005-001

10. CONTRACT GRANT AND/OR PROJECT NO.

11. OTHER DOCUMENT NOS.
DRDKIM System Number: 523184
DRDKIM Accession NUmber: CA025506

12. DOCUMENT RELEASABILITY
Unlimited distribution

13. DOCUMENT ANNOUNCEMENT
Unlimited Announcement

14. ABSTRACT

The human-system interface is central for achieving Network Centric Operations (NCO). Without systems that are designed to be human-centric, NCO will be a 'non starter'. Given this reality, studies of command and control compatibility between human operators and the network are crucial. Without this human oriented focus, unintended consequences will inevitably occur. Unfortunately, this would be just what the gurus of network centric operations were trying to overcome.

L'interface homme-machine est cruciale aux opérations facilitées par réseaux. Sans système centré sur la personne, ces opérations seront vouées à l'échec. Les études sur la compatibilité en matière de commandement et contrôle entre les opérateurs humains et le réseau sont donc essentielles. L'absence de systèmes centrés sur la personne aura inévitablement des incidences non intentionnelles. Malheureusement, ces incidences étaient justement ce que les gourous des opérations facilitées par réseaux tentaient d'éliminer.

15. KEYWORDS, DESCRIPTORS or IDENTIFIERS

Defence R&D Canada

Canada's leader in defence
and national security R&D

R & D pour la défense Canada

Chef de file au Canada en R & D
pour la défense et la sécurité nationale

www.drdc-rddc.gc.ca